네트워크의 물리적 취약요인과 대응기술에 관한 연구

전 정 훈* 안 창 훈** 김 상 춘***

요 약

최근 국내 여러 기반 시설에 USB와 네트워크에 대한 공격이 증가하고 있다. 이러한 공격은 대부분 내부자에 의한 것으로 의도와는 달리, 인위적인 조작에 의해 발생하기도 한다. 이에 따른 인위적 공격의 대응 방안으로 물리보안을 꼽아볼 수 있으며, 대표적인 기술로는 CCTV나 출입통제시스템, 센서 기술이 있다. 그러나 물리보안은 시장성에 따라 몇몇 제품군으로 대표되고 있어, 다양한 물리보안의 기술개발과 확대 적용에 오히려 걸림돌이 되고 있다. 이러한 상황에서 네트워크의 인위적 취약요인으로 인한, 공격이 지속적으로 발생함에 따라, 적절한 물리적 대응기술이 필요한 실정이다. 따라서 본 논문은 물리보안의 인지도와 수요 동향을 알아보고, 네트워크의 물리적 취약요인과 이에 따른 대응기술들을 알아봄으로써, 향후, 국내 물리 보안기술 개발 및 로드맵 구축에 기여할 것으로 기대한다.

Study on the Physical vulnerability factors of network and the Countermeasure technology

Jeon Jeong Hoon* Ahn Chang Hoon** Kim Sang Choon***

ABSTRACT

Recently, The attack on the USB and network are increasing in many domestic infrastructure. These attacks are the most independent of insider intention, caused by the Anthropogenic Manipulation. These attacks are Anthropogenic Response Measures for Physical Security. and Representative Technology has CCTV, Access Control System, Sensor Technology. However, Physical Security, it is represented by several Product family according to the Market, has become an obstacle but rather a variety of Physical Security Technology Development and Application. As the Anthropogenic Attacks have occur continually in the network, it need to the proper Physical Response Techniques in this situation. Therefore, In this paper, we will find out about the awareness and demand trends of Physical Security. And The Physical Vulnerable Factors of Network. Thereby this is expected to be utilized as a basis for the domestic Physical Security Technology development and deployment Road-map in a future.

Key words : Physical vulnerability factors, Physical Security, Industrial Security, Response technology, Anthropogenic Attack

접수일(2016년 12월 08일), 수정일(1차: 2016년 12월 20일), 게재확정일(2016년 12월 27일)

2016년도 강원대학교 대학회계 학술연구조성비로 연구하였음 (관리번호-620160064)

* 동덕여자대학교/컴퓨터학과(책임저자)
** 컴엑스아이/대표이사
*** 강원대학교/정보통신공학전공(교신저자)

1. 서 론

최근 해킹 공격은 온라인 유형뿐만 아니라 오프라인 공격 유형 또한 증가하고 있다. 오프라인 공격은 대부분 내부자의 인위적 조작에 의해 이뤄지고 있으며, 온라인과 병행된 공격들도 시도되고 있다. 이러한 공격을 '사회 공학적 공격(social engineering attack)'으로 부르며, 몇몇 대표되는 기술들을 통해 대응하고 있다. 대표적인 물리 보안기술에는 CCTV(Closed-circuit Television)와 센서(sensor), 출입통제 기술들이 있으며, 규모가 큰 산업현장 및 유동인구가 적은 지역에서 감시 및 모니터링, 통제가 주된 기능들로 사용되고 있다. 그러나 물리보안 기술은 몇몇 대표 제품군으로 분류 및 인지되고 있어 여러 기반시설에 다양한 물리보안의 확대 적용을 방해하고 있다. 예로 국내 물리적 공격유형의 분류 및 제품 등의 통계자료들을 살펴보면, 개발업체들은 다양한 아이디어를 바탕으로 한 기술개발보다도 특정 분야의 상업적 제품에 비중을 두고 있어, 물리보안의 필요성에 대한 인식정도를 알 수 있는 자료도 미흡한 실정이다.

따라서 물리적인 보안 취약점과 필요성에 대한 인식이 다양한 대응기술개발과 물리보안 분야의 활성화에 미치는 영향이 크다 하겠다. 이에 본 논문은 USB와 네트워크의 물리적 취약요인들과 국내 대응기술, 물리보안의 필요성에 대한 설문조사를 통해 위협 동향 및 물리보안의 필요성을 알아보고, 대응기술의 소개 및 방안을 제안함으로써, 향후 다양한 물리보안 기술의 개발 및 확대 적용을 위한 연구 자료로 활용될 수 있을 것으로 기대한다. 본고의 논리적 구성을 위해 2장은 물리보안의 시장성과 수요 동향, 기반시설의 침해사례를 알아보고, 3장은 기반시설의 폐쇄 망에 대한 물리적 취약요인들을 알아본다. 그리고 4장은 물리적 취약요인에 따른 대응 기술 및 방안을 제안하고, 마지막 5장에서 결론 부분으로써 이글을 마치도록 한다.

2. 관련 연구

2.1 물리보안 시장

최근 물리보안 시장의 글로벌 전망에 대해 [1]은 향후 물리보안의 다양한 제품의 확대와 물리보안 시장의 상승세가 지속적으로 이어질 것으로 전망하였다. 그리고 미국의 물리보안 시장에 대해 [2]는 그림1과 같이 지속적인 성장이 예상되고 있는 가운데, 2017년에는 2013년도 대비 약 24%의 상승을 예고하였다.

(그림 1) 미국 물리보안 시장전망(2013~2017년)

또한 글로벌 물리보안 시장의 비중을 살펴보면, 그림2와 같이 아시아 태평양과 서유럽, 북미 순으로 이를 타겟으로 하는 국내 기업들의 CCTV나 출입통제, 인증 제품 등의 해외시장진출이 기대되고 있다[3].

(그림 2) 전 세계 물리보안 시장 비중

그러나 이러한 전망에도 불구하고, 물리보안의 인식 부족과 법률 및 정책 등의 제도적 기반이 마련되지 않을 경우, 앞서 언급된 물리보안 시장의 수요에 미치지 못할 가능성도 배제되어서는 안 될 것이다.

2.2 국내 물리보안 업체 동향

국내 물리보안 제품의 동향을 알아보기 위해 금융감독원의 전자시스템에 관한 자료를 살펴보면, 표1과 같이 국내 업체들은 CCTV와 무인경비, 홈 시큐리티, 토털 시큐리티 등의 제품 및 서비스를 제공하고 있음

을 알 수 있다[4].

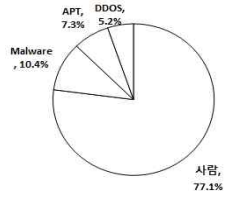
<표 1> 2015년 국내 물리보안업체 및 제품군[4]

물리보안업체	제품군
아이디스	CCTV
ITX시큐리티	CCTV
에스원	무인경비
인론	CCTV
씨앤비텍	CCTV
KT텔레캅	무인경비
코맥스	홈 시큐리티
하이드론씨스템즈	CCTV
한화테크윈	토털 시큐리티

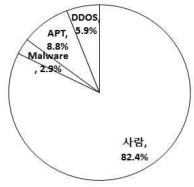
이와 같은 자료를 통해 국내 물리보안 제품들은 CCTV나 무인경비와 이를 응용한 토털 서비스로 구분해 볼 수 있으며, 제품군이 매우 제한적임을 알 수 있다. 따라서 글로벌 경쟁력 강화를 위해서는 다양한 제품군으로 개발범위의 확대와 네트워크와 같은 보안 취약부분에 대한 인위적 공격의 대응기술 개발 등 다양하고, 특화된 서비스가 필요하며, 시장 확대를 위한 중요 요인이 되고 있음을 알 수 있다.

2.3 물리보안의 수요 동향

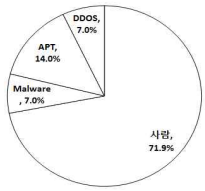
본 절에서는 설문조사내용을 통해 국내 물리보안의 인지도와 수요동향을 알아본다. 설문은 2016년 G-Privacy 컨퍼런스에 참여한 개인정보보호 책임자 및 담당자 168명을 대상으로 물리보안제품의 도입의사와 물리적 보안위협 요인에 대해 설문을 실시하였다. 설문조사 결과는 그림3, 4, 5와 같이 최근 이슈가 되고 있는 정보보안 위협요인들에 대한 보안담당자들의 의견을 기업과 공공기관, 기타로 분류하여 도표로 나타냈다[5]. 이를 살펴보면, 보안 위협요인은 온라인과 사람에 의한 인위적 공격으로 나뉘고 있음을 알 수 있으며, 이에 대해 '기업'은 그림1과 같이 정보보안의 위협요인으로 인적보안을 82.4%로 가장 비중 높았고, 'Malware' 10.4%와 APT 7.3%, DDOS 5.2%, 순으로 나타났다. 또한 그림3과 4의 '공공기관'과 '기타' 설문 결과에서도 각각 82.4%와 71.9%로 '사람'을 보안위협요인으로 가장 높게 꼽았다[5]. 이와 같은 결과를 통해 인위적 보안위협이 점차 높아지고 있으며, 적절한 대응방안 마련이 필요함 시사하고 있음을 알 수 있다.



(그림 3) 정보보안의 위협요인(기업)

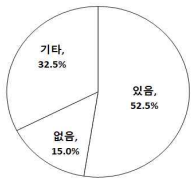


(그림 4) 정보보안의 위협요인(공공기관)

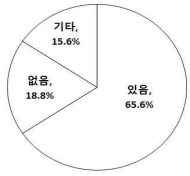


(그림 5) 정보보안의 위협요인(기타)

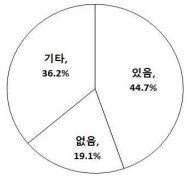
물리보안 제품에 대한 도입 의향을 묻는 질문에는 그림6, 7, 8과 같이 '기업'은 52.5%가 '도입의향이 있음'을 나타냈고, '공공기관'과 '기타'에서는 각각 65.6%, 44.7%로 도입 의향이 '있음'을 나타냈다[5].



(그림 6) 물리보안 제품도입의향(기업)



(그림 7) 물리보안 제품도입의향(공공기관)



(그림 8) 물리보안 제품도입의향(기타)

이러한 결과는 점차 온라인 공격보다 인위적인 공격이 가장 큰 위협으로 작용하고 있으며, 이에 따른 대응기술의 필요성 인식이 개선되고 있음을 알 수 있다. 자료를 종합해보면, 최근 온라인 공격이 급증하고 있음에도 기업과 공공기관은 '사람'을 가장 큰 위협요인으로 꼽고 있으며, 다양한 대응 기술들이 있는 온라인 보다는 상대적으로 미흡함을 알 수 있다. 그리고 도입의사를 묻는 질문에 '있음'의 비중이 매우 높은 원인은 이에 따른 적절한 대응 방안이 부재함을 상대적으로 반증하고 있음을 알 수 있다.

2.4 기반시설의 물리적 침해 사례

(그림 9) 주요 사회기반시설공격사례[7]

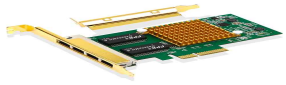
최근 기반시설에서는 USB와 내부 네트워크의 사용을 악용한 공격들이 발생하고 있어, 이에 따른 물리적 공격사례들을 알아본다. [6]과 [7]에 따르면 국내 기반시설들은 폐쇄망으로 이뤄진 경우가 대부분으로 공격자는 USB의 사용 및 내부 네트워크의 접근을 주 공격경로로 악용하고 있음을 언급하고 있으며, 이러한 최근 공격사례들을 그림9를 통해 글로벌하게 발생되고 있음을 알 수 있다. 한편 국내의 침해 사례로는 2011년4월 발생한 농협 해킹사건을 꼽아 볼 수 있는데 이 사건은 서버 유지보수 업체직원이 감염된 노트북을 전산망 내부에서 사용함으로써, 직원의 노트북을 좀비 PC로 사용하여 정보가 유출된 사건으로 외부에서 사용하던 시스템을 내부 네트워크에서 인위적으로 변칙 사용함으로 인해 발생한 사례 중에 하나이다[8]. 그리고 2013년 발생한 KB 국민카드와 NH 농협카드, 롯데카드의 경우에도 KCB 신용 평가사 직원에 의해 개발 작업 중, 시스템 테스트를 위해 받은 개인정보를 USB에 담아 유출된 사례가 있다[9]. 이와 같은 사고사례들은 모두 네트워크 및 USB 포트를 악용한 대표적인 사례들이다.

3. 폐쇄 망 내에서의 물리적 취약요인

최근 기반시설에서 발생하고 있는 사고사례들의 대부분이 USB나 내부 네트워크의 사용이 주요 원인이 되고 있는 가운데, 공격자는 역추적이나 증적자료의 확보를 피하고 있어, 이에 대한 대응이 매우 어려운 실정이다. 따라서 기반시설에서 발생하고 있는 네트워크의 물리적 공격에 따른 취약요인들을 알아본다.

3.1 유선 네트워크

유선 네트워크의 연결은 시스템에 내장된 네트워크 카드의 포트를 사용하거나, 그림10과 같은 다중 포트의 네트워크 카드를 추가 장착함으로써 쉽게 사용이 가능하다.



(그림 10) 유선 네트워크 카드[10]

다중 포트 네트워크 카드는 표현 그대로 다중 연결을 용이하게 함으로써, 주로 중·대형 급 시스템에서 사용되고 있지만, 미사용 포트는 오히려 네트워크의 취약요인이 되고 있다. 또한 공격자는 사용 중인 포트의 인위적 변경으로 내부망의 침입을 용이하게 한다. 따라서 유선 네트워크 카드의 사용하지 않는 네트워크 포트나 사용 중인 포트에 대한 대응이 요구된다.

3.2 무선 네트워크

무선 네트워크는 와이파이(wifi)를 비롯해 블루투스(bluetooth), NFC(near field communication) 등 다양한 기술들이 있다. 이와 같은 기술들은 시스템에 내장되거나, 그림11, 12와 같이 USB 단자 형태의 장치(네트워크 카드 또는 동글:dongle)를 통해 유·무선 장비에 사용이 용이하다.

(그림 11) USB 모듈[11]

(그림 12) 동글 [12]

그러나 무선 네트워크는 그림9와 10처럼 무선 장치를 추가함으로써 쉽게 접근이 가능하기 때문에, 접근을 제한하기 위해 SSID(service set identifier)와 같은 인증체계를 사용하고 있지만, 무선 데이터의 스니핑(sniffing) 공격이나 SSID의 크랙(crack) 등에 매우 취약한 단점이 있다. 특히 내부자에 의한 무선 네트워크의 공격은 매우 치명적이어서, 이에 따른 무선 네트워크의 인위적 공격의 대응이 필요하다.

3.3 네트워크 중계 장치

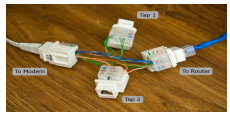
네트워크는 중계 장치를 통해 확장 및 분할하기 위해, 그림13과 같이 여러 포트를 장착하고 있다. 그러나 미사용 포트의 경우, 인위적인 악용이 가능하며, 기존에 사용하는 포트를 이용해 공격에 악용될 수 있다. 특히 네트워크의 효율적이 관리를 위해 DHCP(Dynamic Host Configuration Protocol) 서버를 통한 네트워크 주소의 자동할당은 공격자가 IP주소를 알아낼 필요 없이 네트워크 라인만 연결하면, 공격 시스템에 주소를 자동할당 받을 수 있기 때문에 내부 네트워크로의 접근이 용이하다.

(그림 13) 스위치[13]

이에 네트워크 주소를 통한 사용제한 방법이 있으나, 내부자에 의한 공격에는 취약한 단점이 있다. 결과적으로 내·외부 자에 의한 네트워크 중계 장치의 인위적 공격위협은 증적자료를 통한 역추적이 어려워 이에 따른 대응이 요구된다.

3.4 라인 탭핑

유선 네트워크는 다중 기기의 연결을 위해 회선을 분기하기 위해 그림14와 같이 '탭핑' 사용하지만, 이러한 '라인 탭핑'은 회선 분기의 목적이 아닌 공격수단으로 악용되고 있어 이에 따른 대응이 요구된다.



(그림 14) 라인 탭핑[14]

따라서 시스템 또는 네트워크 중계 장비의 사용 중이거나 미사용 중인 포트를 이용한 공격에 취약하기 때문에 이에 대한 인위적인 공격의 대응이 필요하다.

4. 대응 방안

최근 원자력발전소와 같은 기반시설 등의 공격경로가 대부분 USB나 내부 네트워크의 접근을 악용해 발생하고 있다[6][7]. 따라서 이와 같은 인위적 위협들에 대해 3장에서 언급한 취약요인들의 대응방안을 제안하고자 한다.

4.1 사용 중인 포트에 대한 위협 대응

네트워크 포트는 공격자에게 인위적인 사용을 사실상 허용하고 있어, 내부 망으로의 침입을 가능하게 하며, 이에 따른 증적자료도 남지 않아 역추적이 어려운 취약점이 있다.

(그림 15) 링크 락

(그림 16) 랜 케이블 락

따라서 인위적 공격을 원천 차단하기 위해서는 그림15, 16과 같은 물리적 잠금 장치들을 사용해 사용

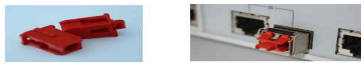
중인 회선의 안정성 유지와 '라인 변경'에 의한 공격을 예방할 수 있다. 그림15와 같이 RJ45에 사용 중인 네트워크 라인의 인위적인 변경을 방지하도록 물리적인 잠금장치를 통해 불법적인 사용을 차단하고, 동일 장치를 통해 인위적인 네트워크 라인의 분리를 방지함으로써, 내부자에 의한 공격에 대응할 수 있다.

4.2 미사용 포트에 대한 위협 대응

시스템과 중계 장치의 사용하지 않는 통신포트(USB포트 등)는 인위적인 공격에 매우 취약하다. PC의 경우, 다중 네트워크 포트에 대해 인위적인 공격과 USB포트를 이용한 장치들을 통한 공격이 용이하기 때문에 이에 따른 공격 대응방안이 필요하다.

(그림 17) 포트 폐쇄 락

(그림 18) USB 포트락



(그림 19) 광 포트 락

이에 그림17과 같이 포트를 폐쇄하는 잠금 장치의 사용으로 인위적이며, 의도적인 악용을 예방할 수 있다. USB형태의 각종 통신기기나 광 단자는 그림18, 19와 같이 잠금 장치를 사용함으로써, 인위적인 변경 및 악용에 대응할 수 있다.

4.3 네트워크 중계 장치의 위협 대응

네트워크 중계 장치는 다수의 시스템을 연결하기 위해 여러 포트들로 구성되어 있다. 그러나 연결 상황에 따라 미사용 포트에 대해 인가되지 않은 시스템의 사용이 가능하기 때문에 이를 이용한 공격이 가능하다.

(그림 20) 링크 락용 HUB

그림20과 같이 네트워크의 연결을 제한하기 위해 앞서 그림15의 장치를 HUB에 연결함으로써, 특정 네트워크 포트에 대한 사용을 제한할 수 있다. 특히 내부자에 의한 네트워크의 인위적 공격의 취약점은 증적자료 및 로그 기록만으로 역추적이 어렵고, 사람에 의한 공격에 대응하기 어렵기 때문에, 앞서 언급된 물리적 보안장치들을 통해 공격을 사전 예방함으로써, 추후 피해를 줄이고, 정보자산을 지킬 수 있을 것으로 기대한다.

5. 결 론

최근 IoT기술의 보급으로 유·무선 네트워크에 대한 인위적인 공격이 증가가 예상되고 있는 가운데, 응용분야인 기반시설의 경우, 내부자에 의한 공격대응이 매우 어려운 실정이다. 이에 내부자에 의한 인위적인 공격에 가장 효과적인 대응 방안으로 물리적 보안을 꼽아 볼 수 있다. 대표적인 기술로는 CCTV나 출입통제 시스템 등이 있으며, 최근 물리적 보안 분야의 지속적인 성장이 기대되고 있다. 그러나 이러한 상황과는 반대로 시장성이 높은 제품 중심의 홍보 및 개발로 인해, 다양한 물리보안 기술의 개발 및 확대에 오히려 걸림돌이 되고 있다.

따라서 본 논문은 최근 물리보안시장의 동향과 제품의 수요 동향, 침해사례를 통해 원인을 알아보고, 네트워크의 물리적 취약요인에 대한 다양한 대응기술들을 알아봄으로써, 물리보안의 다양한 기술 소개와 필요성 인식, 대책 마련 등에 유용한 자료로 활용될 수 있을 것으로 기대한다. 그러나 향후, 다양한 물리보안 기술의 개발 및 확대 적용을 위해 물리적 보안위협요인에 대한 체계적인 연구를 통해 대응 방안의 마련 및

지속적인 기술개발이 필요할 것으로 사료된다.

참고문헌

[1] 전정훈, “융합 IT환경의 물리적 취약요인에 관한 연구,” 한국융합보안학회, vol.16, no.1, 2016.

[2] 전정훈, “사물인터넷의 기술 동향과 전망에 관한 연구,” 한국융합보안학회, vol.14, no.7, 2014.12

[3] 전정훈, “사물인터넷의 보안 위협 요인들에 대한 분석,” 한국융합보안학회, vol.15, no.7, 2015.12

[4] 물리보안업체 매출현황 http://www.boannews. com/media/view.asp?idx=47818

[5] 안창훈, “2016년 G-Privacy 컨퍼런스 개인정보보호책임자 및 담당자에 대한 설문조사자료,” 컴액스아이, 2016.4

[6] 디지털타임스, “USB로 국가 기반시설 뚫린다.”, http://www.dt.co.kr/contents.html?article_no=2010110102010560746005

[7] 안랩, “사회기반시설 공격 동향 분석보고서,” 시큐리티대응센터 분석팀, 2016.5

[8] 디지털타임스 “안철수 연구소 최신보안 뉴스,” http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?cmd=print&seq=17712&menu_dist=1

[9] “카드 3사 고객 신용정보 유출,” http://www.newsquare.kr/issues/39

[10] https://ae01.alicdn.com/kf/HTB1QnteIpXXXXaSXFXXq6xXFXXXi/High-Quanlity-I350-T4-PCI-E-Server-Adapter-Gigabit-LAN-Gigabit-NIC-font-b-Network-b.jpg

[11] http://www.betanews.net/imagedb/orig/2010/0121/02ea 79fe.jpg

[12] http://timg.danawa.com/prod_img/500000/659/336/img /133 6659_1.jpg

[13] http://cfile236.uf.daum.net/image/024FAA3350980E851D 0577

[14] http://3.bp.blogspot.com/-PjpEpicX6qE/UXR3jU7xDlI/AAAAAAAACB4/ZrmOLHLZx_c/s1600/tap.jpg

[著者紹介]

전 정 훈 (Jeong-hoon Jeon)

2008년 2월 숭실대학교 일반대학원 컴퓨터학과 공학박사
2005년 5월~ 현 동덕여자대학교 컴퓨터학과 교수

email : nerdrandy@dongduk.ac.kr

안 창 훈(Chang-Hoon An)

1998년 2월 경기대 무역학과 졸
2001년 ~ 현재: 컴엑스아이 대표
2008년 ~ 2013년: KPC 전문위원

e-mail :cosmohoon@comxi.com

김 상 춘(Sang-Choon Kim)

1999년 8월 충북대 이학박사
1983년 ~ 2001년: ETRI 선임
2001년 ~ 2010년: ETRI초빙연구원
2001년 ~ 현 강원대학교 정교수

e-mail : kimsc@kangwon.ac.kr